



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/904,310	07/11/2001	Handong Wu	NETAP011	2093
28875	7590	12/06/2004	EXAMINER	
Zilka-Kotab, PC			JEAN GILLES, JUDE	
P.O. BOX 721120			ART UNIT	PAPER NUMBER
SAN JOSE, CA 95172-1120			2143	

DATE MAILED: 12/06/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

## Office Action Summary

**Application No.**

09/904,310

**Applicant(s)**

WU ET AL.

**Examiner**

Jude J Jean-Gilles

**Art Unit**

2143

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☐ Responsive to communication(s) filed on 11 July 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-29 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-29 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 11 July 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- |   |   |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)  | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date <u>01/11/02</u> . | 6) <input type="checkbox"/> Other: _____  |

JG.

### **DETAILED ACTION**

This office action is responsive to communication filed on 07/11/2001. Claimed priority is granted from provisional application No. 60264598 with an effective filing date of 01/26/2001.

#### ***Information Disclosure Statement***

1. The references listed on the Information Disclosure Statement submitted on 01/11/2002 have been considered by the examiner (see attached PTO-1449A).

#### ***Claim Rejections - 35 USC § 102***

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1-4, 15-16, and 20-24 are rejected under 35 U.S.C. 102(e) as being unpatentable by Redlich (U.S. Patent No. 6,591,306 B1).

**Regarding claim 1:** Redlich teaches a method for protecting a host located within a computer network (*fig. 18, items 200, 210, 400, 502-503, and 900*), the method comprising:

Art Unit: 2143

mapping a public host address for a public host to a secret host address for a secret host containing data accessible over the computer network (*column 16, lines 15-24; note that the guess station is the public host and that the local stations are the local hosts*), said public host address being available from a domain name system server (*column 28, lines 47-52; note that appointment of a couple of DNS servers on the guest's home network*);

receiving a request for communication with the secret host at the public host (*column 18, lines 57-67; column 19, lines 1-10*);

forwarding said request from the public host to the secret host (*column 19, lines 11-15*); and

processing said request at the secret host and communicating from the secret host over the network, wherein said communication appears to be sent from the public host (*column 20, lines 25-36*).

**Regarding claim 2:** Redlich teaches the method of claim 1 wherein the network is the Internet and the secret host is a server (*fig. 19, items 900, 941-942; column 18, lines 48-56; column 28, lines 56-64*).

**Regarding claim 3:** Redlich teaches the method of claim 2 wherein the server hosts a Web site (*column 29, lines 49-59*).

**Regarding claim 4:** Redlich teaches the method of claim 1 wherein receiving a request comprises receiving a URL at the domain name system server, the domain name system server providing an IP address of the public host corresponding to the URL (*column 29, lines 49-59*).

Art Unit: 2143

**Regarding claim 15:** Redlich teaches a computer program product for protecting a host located within a computer network (*fig. 18, items 200, 210, 400, 502-503, and 900*), comprising:

computer code that maps a public host address for a public host to a secret host address for a secret host containing data accessible over the computer network (*column 18, lines 16-26*), said public host address being available from a domain name system server (*column 28, lines 47-52; fig. 11, tunnel server*);

computer code that receives a request for communication with the secret host at the public host (*column 18, lines 16-34*);

computer code that forwards said request from the public host to the secret host (*column 18, lines 16-34*);

computer code that processes said request at the secret host and communicates from the secret host over the network, wherein said communication appears to be sent from the public host (*column 18, lines 16-37*); and

a computer-readable storage medium for storing the codes (*column 18, lines 25-27*).

**Regarding claim 16:** Redlich teaches the computer program product of claim 15 wherein the computer readable medium is selected from the group consisting of CD-ROM, floppy disk, tape, flash memory, system memory, hard drive, and data signal embodied in a carrier wave (*column 18, lines 25-27*).

Art Unit: 2143

**Regarding claim 20:** Redlich teaches a system for protecting a host located within a computer network (*fig. 18, items 200, 210, 400, 502-503, and 900*), the system comprising:

a public host having a public host address available from a DNS server (*column 28, lines 47-52*); and

a secret host having a secret host address and containing data accessible over the computer network, said public host address being mapped to said secret host address (*column 16, lines 15-24*);

wherein the public host is operable to forward requests received from the network to the secret host and the secret host is Operable to process said requests and communicate from the secret host to the network with said communication appearing to be sent from the public host (*column 20, lines 25-36; column 19, lines 1-15*).

**Regarding claim 21:** Redlich teaches the system of claim 20 wherein the secret host is configured to manage the public host (*column 3, lines 62-67*).

**Regarding claim 22:** Redlich teaches a method for hiding an IP address of a computer node located within a computer network (*fig. 18, items 200, 210, 400, 502-503, and 900*), the method comprising:

associating an IP address for a public node with an IP address of a secret node such that only the public node has access to the IP address of the secret node, said P address for the public node being available from a DNS server (*column 28, lines 47-52; note that appointment of a couple of DNS servers on the guest's home network*);

Art Unit: 2143

receiving packets from the network at the public node (*column 18, lines 57-67; column 19, lines 1-10*);

forwarding said packets from the public node to the secret node (*column 19, lines 11-15*); and

responding to said packets at the secret node such that a response appears to be sent from the public node rather than the secret node (*column 20, lines 25-36*).

**Regarding claim 23:** Redlich teaches the method of claim 22 wherein the packets contain requests for data and the secret node is a server hosting a Web site (*fig. 19, items 900, 941-942; column 28, lines 56-64; column 29, lines 49-59*).

**Regarding claim 24:** Redlich teaches the method of claim 22 wherein the packets contain e-mail (*column 16, lines 45-51*).

***Claim Rejections - 35 USC § 103***

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 5-14, 17-19, and 25-29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Redlich (U.S. Patent No. 6,591,306 B1) in view of Underwood (U.S. 6,704,873 B1).

**Regarding claim 5:** Redlich discloses the invention substantially as claimed. Redlich teaches the method for protecting a host located within a computer network of claim 1. However, Redlich is silent on having the method of claim 1, wherein forwarding said request comprises slowing down the forwarding of requests when the public host identifies an attack.

In the same field of endeavor, Underwood discloses "*an Internet screening router that denies typical attacks caused by malicious manipulation of EP options flag such as source routing and fragmentation attacks. Note that the denial of data packets will automatically slow down the system.*" [see Underwood; column 284, lines 48-50].

Accordingly, it would have been obvious to one of ordinary skill in the networking art at the time the invention was made to have incorporated Underwood's teachings of slowing down the forwarding of request packets with the teachings of Redlich, for the purpose of improving the ability of a local



Art Unit: 2143

network *"to provide for security against malicious intrusion or attacks from a foreign network"* as stated by Redlich in lines 34-36 of column 14.

**Regarding claim 6:** Redlich discloses the invention substantially as claimed. Redlich teaches the method for protecting a host located within a computer network of claim 1. However, Redlich is silent on having the method of claim 1, further comprising stopping the forwarding of said request when the public host identifies an attack.

In the same field of endeavor, Underwood discloses *"a screening router that blocks all ICMP packets to prevent many well known attacks like the Ping of Death. Note that blocking the sending of data packets will automatically slow down the system."* [see Underwood; column 284, lines 51-55].

Accordingly, it would have been obvious to one of ordinary skill in the networking art at the time the invention was made to have incorporated Underwood's teachings of stopping the forwarding of request packets with the teachings of Redlich, for the purpose of improving the ability of a local network *"to provide for security against malicious intrusion or attacks from a foreign network"* as stated by Redlich in lines 34-36 of column 14.

**Regarding claim 7:** The combination Redlich-Underwood teaches the method of claim 6 further comprising notifying the secret host of the attack [see Underwood, column 266, lines 44-47; note the inclusion of various products to support notification of an attack]. By this rationale **claim 7** is rejected.

**Regarding claim 8:** The combination Redlich-Underwood teaches the method of claim 7 further comprising tracking down a source of the attack [see *Underwood, column 267, lines 64-65*]. By this rationale **claim 8** is rejected.

**Regarding claim 9:** The combination Redlich-Underwood teaches the method of claim 8 wherein tracking down a source of the attack comprises performing a trace back at the secret host [see *Underwood, column 266, lines 44-47; note the inclusion of various products to support notification of an attach which includes tracing the source of the attack*]. By this rationale **claim 9** is rejected.

**Regarding claim 10:** Redlich discloses the invention substantially as claimed. Redlich teaches the method for protecting a host located within a computer network of claim 1. However, Redlich is silent on having the method of claim 1, further directing one or more clients to send requests to an alternate public host.

In the same field of endeavor, Underwood discloses "*some local users may choose to circumvent the security systems and mechanism by choosing an alternate path to the guest hosts...*" [see *Underwood; column 283, lines 46-48*].

Accordingly, it would have been obvious to one of ordinary skill in the networking art at the time the invention was made to have incorporated Underwood's teachings using alternate paths to send requests with the teachings of Redlich, for the purpose of improving the ability of a local network "*to provide for security against malicious intrusion or attacks from a foreign network*" as stated by Redlich in lines 34-36 of column 14.

**Regarding claim 11:** The combination Redlich-Underwood teaches the method of claim 10 wherein a notification that the public host is under attack is received at the secret host [see *Underwood*, column 226, lines 49-50; column 228, lines 35-37]. By this rationale **claim 11** is rejected.

**Regarding claim 12:** The combination Redlich-Underwood teaches the method of claim 10 wherein a notification that the public host is congested is received at the secret host [see *Underwood*, column 228, lines 45-46]. By this rationale **claim 12** is rejected.

**Regarding claim 13:** The combination Redlich-Underwood teaches the method of claim 10 wherein the secret host has received a request for heightened security [see *Redlich*, column 25, lines 19-22]. By this rationale **claim 13** is rejected.

**Regarding claim 14:** The combination Redlich-Underwood teaches the method of claim 10 further comprising requesting the DNS server to replace the public host address with an alternate public host address [see *Redlich*, column 23, lines 34-63]. By this rationale **claim 14** is rejected.

**Regarding claim 17:** Redlich discloses the invention substantially as claimed. Redlich teaches the computer program product of claim 15. However, Redlich is silent on having the computer program product of claim 15 further comprising code that receives at the secret host a notification that the public host is under attack.

In the same field of endeavor, Underwood discloses that "*if anything suspicious in the nature of an attack is observed, the firewall may notify an*

Art Unit: 2143

*operator of a problem (local node) and shut itself down if possible” [see Underwood; column 284, lines 35-37].*

Accordingly, it would have been obvious to one of ordinary skill in the networking art at the time the invention was made to have incorporated Underwood’s teachings using computer code to notify an attack on a public host in a local network with the teachings of Redlich, for the purpose of improving the ability of a local network *“to provide for security against malicious intrusion or attacks from a foreign network”* as stated by Redlich in lines 34-36 of column 14.

**Regarding claim 18:** The combination Redlich-Underwood teaches the computer program product of claim 17 further comprising code that directs one or more clients to send requests to an alternate public host upon receiving said notification [*see Redlich, column 24, lines 53-57*]. By this rationale **claim 18** is rejected.

**Regarding claim 19:** The combination Redlich-Underwood teaches the computer program product of claim 17 further comprising code that requests the DNS server to replace the public host address with an alternate public host address upon receiving said notification [*see Redlich, column 24, lines 53-57*]. By this rationale **claim 19** is rejected.

**Regarding claim 25:** Redlich discloses the invention substantially as claimed. Redlich teaches the method of hiding an IP address of claim 22. However, Redlich is silent on having method of claim 22 further comprising stopping the forwarding of packets when the public node is under attack.

In the same field of endeavor, Underwood discloses *"a screening router that blocks all ICMP packets to prevent many well known attacks like the Ping of Death. Note that blocking the sending of data packets will automatically slow down the system."* [see Underwood; column 284, lines 51-55].

Accordingly, it would have been obvious to one of ordinary skill in the networking art at the time the invention was made to have incorporated Underwood's teachings of blocking the forwarding of request packets with the teachings of Redlich, for the purpose of improving the ability of a local network *"to provide for security against malicious intrusion or attacks from a foreign network"* as stated by Redlich in lines 34-36 of column 14.

**Regarding claim 26:** The combination Redlich-Underwood teaches the method of claim 25 further comprising requesting the DNS server to replace the IP address of the public node with an IP address of an alternate public node [see Redlich, column 23, lines 34-63]. By this rationale **claim 26** is rejected.

**Regarding claim 27:** The combination Redlich-Underwood teaches the method of claim 25 further comprising directing specific client computers to send packets directed at the public node to an alternate public node [see Underwood; column 283, lines 46-48]. By this rationale **claim 27** is rejected.

**Regarding claim 28:** The combination Redlich-Underwood teaches the method of claim 22 further comprising switching to an alternate public host when congestion at the public host exceeds a predetermined level. [see Underwood, column 228, lines 45-46]. By this rationale **claim 28** is rejected.

Art Unit: 2143

**Regarding claim 29:** The combination Redlich-Underwood teaches the method of claim 22 further comprising switching to an alternate public host to provide increased security at the secret host [see *Redlich*, column 25, lines 19-22]. By this rationale **claim 29** is rejected.

### ***Conclusion***

6. Any inquiry concerning this communication or earlier communications from examiner should be directed to Jude Jean-Gilles whose telephone number is

Art Unit: 2143

(571) 272-3914. The examiner can normally be reached on Monday-Thursday and every other Friday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, David Wiley, can be reached on (571) 272-3923. The fax phone number for the organization where this application or proceeding is assigned is (703) 305-3719.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

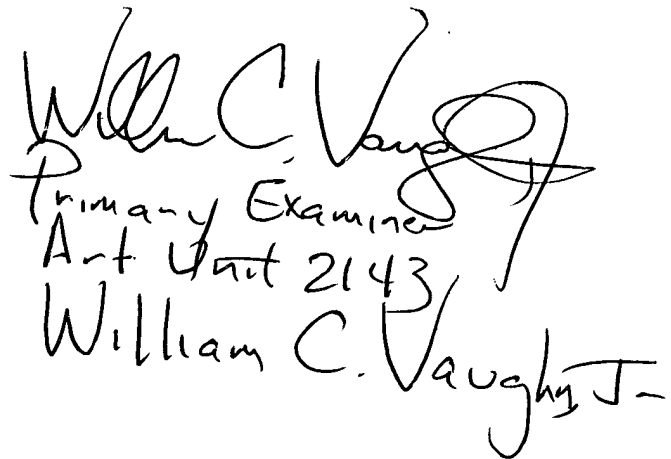
Jude Jean-Gilles

Patent Examiner

Art Unit 2143

JJG

November 23, 2004



William C. Vaughn  
Primary Examiner  
Art Unit 2143  
William C. Vaughn, Jr.